(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organizati n
International Bureau

(43) International Publication Date
19 July 2001 (19.07.2001)

PCT

(10) International Publication Number
WO 01/52234 A1

(51) International Patent Classification[7]: G10H 1/00, G06F 1/00

(21) International Application Number: PCT/EP00/13227

(22) International Filing Date:
27 December 2000 (27.12.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/176,074 13 January 2000 (13.01.2000) US
09/636,725 11 August 2000 (11.08.2000) US

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor: EPSTEIN, Michael; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: GROENENDAAL, Antonius, W., M.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

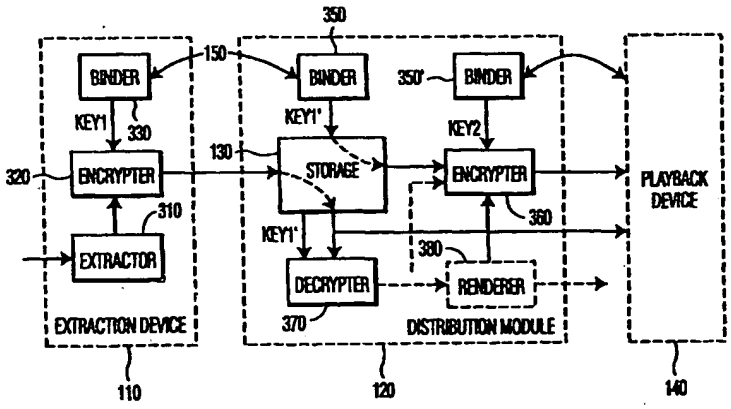
(81) Designated States *(national)*: CN, JP, KR.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: PROTECTING COMPRESSED CONTENT AFTER SEPARATION FROM ORIGINAL SOURCE



(57) Abstract: The device that legitimately extracts content material from a source is bound to the compliant module that enforces copy protection schemes in the distribution of copy protected material. The extraction device (110) thereafter binds the extracted content material to the compliant module (120) that enforces copy protection. By binding the legitimate extractor (110) to the distribution module (120) that enforces copy protection, other, potentially unauthorized, extractions from other extraction devices, can be distinguished. Because the binding of the legitimate extractor (110) to the distribution module (120) is used to distinguish legitimate extractions, rather than encoding characteristics of the extracted content, such as the presence or absence of a fragile watermark, the legitimate extractor (110) can be configured to provide any encoding, including compressed encodings that minimize bandwidth and memory requirements. The binding of the extraction device (110) to the distribution module (120) can be physical or logical. A physical binding relies on the physical integrity of the system to assure that alternative sources cannot gain access to the distribution module (120). A logical binding relies on cryptographic techniques to assure that only authorized extractors (110) are bound to distribution modules (120).

WO 01/52234 A1

Protecting Compressed Content after Separation from Original Source

This application claims the benefit of U.S. Provisional Application No. 60/176,074 filed 13 January 2000, Attorney Docket US000007P.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates primarily to the field of consumer electronics, and in particular to the protection of copy-protected content material.

2. Description of Related Art

A number of systems have been proposed for protecting content material, such as an audio or video recording, from unauthorized copying and unauthorized distribution. The Secure Digital Music Initiative (SDMI) and others advocate the use of a "licensed compliant module" (LCM) to control the recording and distribution of the protected material. The LCM typically stores the protected material in a local storage device in a secure form, such as an encrypted form. When the user desires to provide another device, such as a portable playback device (PD), with the content material, the LCM verifies that the PD is a compliant device, and provides the content material to the device, subject to agreed upon, or licensed, conditions. In a typical embodiment, the LCM includes a check-in/check-out process, wherein a log is maintained for each copy of each protected material that is provided to a PD. When the PD "checks-in" the material, the material is erased from the PD, and the log is updated. If the protected material, for example, includes a "one copy at a time" restriction, the LCM will not provide another copy of the protected material until a prior copy is returned.

A variety of techniques have been proposed for assuring that the LCM only receives and stores authorized copies of the protected material. These security techniques have primarily focused on providing a means of distinguishing unauthorized copies of material that are distributed via the Internet. Generally, material that is distributed via the Internet is distributed in a compressed form, to minimize the bandwidth requirements for

downloading the material, and at least one security system is based on the detection of a compressed format, or the detection of an uncompressed format that had been compressed.

The Secure Digital Music Initiative and others advocate the use of "digital watermarks" to identify authorized content material. EP 0981901 "Embedding auxiliary data in a signal" issued 1 March 2000 to Antonius A.C.M. Kalker, discloses a technique for watermarking electronic material, and is incorporated by reference herein. As in its paper watermark counterpart, a digital watermark is embedded in the content material so as to be detectable, but unobtrusive. An audio playback of a digital music recording containing a watermark, for example, will be substantially indistinguishable from a playback of the same recording without the watermark. A watermark detection device, however, is able to distinguish these two recordings based on the presence or absence of the watermark. A "robust" watermark can not be removed from the content material without destroying the content material. Conversely, a "fragile" watermark, as its name implies, is a watermark that is destroyed or damaged if any changes are made to the content material. By encoding protected material with a robust and a fragile watermark, an LCM can detect that the material is protected material (via the presence of the strong watermark), and can also detect whether the material had ever been compressed or otherwise tampered with (via the absence of the weak watermark).

This fragile-watermarking protection, however, assumes that all authorized copies of content material will be in an uncompressed form. With the popularity of compressed formats becoming more prevalent, however, consumer devices are being produced that provide compressed format outputs. For example, application programs on personal computers are available that read Compact Discs (CDs) and store the songs from the CD onto a hard drive storage unit in compressed form, commonly MP3. Similarly, CD players are available, or will soon be available, with direct MP3 or similar output for the digital transfer of songs to other devices, such as an LCM. In this scenario, a user's authorized copy of a song from a CD that the user has purchased will be indistinguishable from an unauthorized copy of a song from the Internet, because both copies will have a robust watermark, but no fragile watermark.

BRIEF SUMMARY OF THE INVENTION

It is an object of this invention to provide a method and system for protecting content material from unauthorized copying and/or distribution after this content material is removed or copied from its original source. It is a further object of this invention to provide a

method and system for distinguishing locally produced compressed files from files that are distributed from a remote source, such as an Internet site.

These objects and others are achieved by binding the device that legitimately extracts content material from a source to the compliant module that enforces copy protection schemes in the distribution of copy protected material. Thereafter, the device that extracts the content material binds the content material to the compliant module that enforces the copy protection schemes. By binding the legitimate extractor to the distribution module that enforces copy protection, other, potentially unauthorized, extractions from other extraction devices, can be distinguished. Because the binding of the legitimate extractor to the distribution module is used to distinguish legitimate extractions, rather than encoding characteristics of the extracted content, such as the presence or absence of a fragile watermark, the legitimate extractor can be configured to provide any encoding, including compressed encodings that minimize bandwidth and memory requirements. The binding of the extraction device to the distribution module can be physical or logical. A physical binding relies on the physical integrity of the system to assure that alternative sources cannot gain access to the distribution module. A logical binding relies on cryptographic techniques to assure that only authorized extractors are bound to distribution modules.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is explained in further detail, and by way of example, with reference to the accompanying drawings wherein:

FIG. 1 illustrates an example block diagram of a secure extraction and distribution system in accordance with this invention.

FIG. 2 illustrates an example block diagram of an alternative secure extraction and distribution system in accordance with this invention.

FIG. 3 illustrates an example block diagram of an extraction device and distribution module that provides secure communication of content material in accordance with this invention.

Throughout the drawings, the same reference numerals indicate similar or corresponding features or functions.

DETAILED DESCRIPTION OF THE INVENTION

FIG. 1 illustrates an example block diagram of a secure extraction and distribution system 100 in accordance with this invention. The system 100 includes a

compliant extraction device 110 and a compliant distribution module 120. A "compliant" component is one that conforms to the security protocols established, such as conforming to the SDMI specifications. For example, a compliant extractor determines the distribution and copy limits associated with original source material, extracts portions of the content material only if authorized, and communicates any distribution or copy limits along with each extraction. In SDMI terminology, the extraction device 110 is commonly referred to as a "ripper", and the distribution module 120 as a "Licensed Control Module", or "LCM". The extraction device 110 is configured to extract one or more data items from a source 101 of protected or unprotected data. In the context of this invention, the extraction and processing of protected data is discussed hereinafter.

In the context of SDMI, the extracted data item is an extraction of one or more songs from an album on a CD or other media. The distribution module 120 is configured to facilitate maintaining a collection of data items, e.g. songs, on a local storage device 130, and to facilitate the distribution of the individual data items to other devices 140, typically portable or stationary playback devices. In other contexts, the distribution module 120 may also be configured to facilitate the distribution of the data items to other recording devices or other distribution systems. Copending U.S. patent application "NEW PROTOCOL FOR SECURE REGISTRATION OF MUSIC (or any data) IN A CHECK IN CHECK OUT SYSTEM", serial number 09/548,728, filed 13 April 2000 for Michael Epstein, Attorney Docket PHA-23,671 describes a method and system for limiting the distribution of protected content material among playback devices to conform to licensed distribution rights, and is incorporated by reference herein.

In accordance with a first aspect of this invention, the extraction device 110 and the distribution module 120 are bound together, such that the extraction device 110 only provides extracted data item(s) that are bound to a compliant distribution module 120, and a distribution device 120 only accepts data items that are bound to it via a compliant extraction device 110.

A compliant component contains a means of identifying itself as a compliant component. Typically, a compliant component contains an identifier that is 'certified' by a "trusted authority". The trusted authority digitally signs the certificate that identifies the compliant component, using a private key that is known only to the trusted authority. In accordance with this invention, the compliant components 110, 120 also include a public key of the trusted authority that is used to verify the digital signature, and the identifier of each device corresponds to a public key that is associated with each component 110, 120. Each

component 110, 120 also contains a private key corresponding to the certified public key, as a public-private key pair, common in the art.

To logically bind the two components 110, 120 together, a cryptographic authentication process is used, as illustrated by the bi-directional arrow 150. Each component 110, 120 communicates, via 150, its certified public key to the other 120, 110, and each component 110, 120 verifies that the communicated public key has been certified by the trusted authority. To verify that the other component is the compliant component that is identified by the certificate, a challenge-response protocol is used. The first component transmits a random number to the second component (the challenge). The second component encrypts the random number using its private key, and transmits the encrypted number back to the first component (the response). The first component decrypts the encrypted number, using the second component's certified public key. If the decryption of the encrypted number matches the originally transmitted random number, the second component is verified as being the certified component, because only the second component has knowledge of the private key corresponding to its certified public key. This challenge-response process is then repeated by the second component, to verify that the first component is the component corresponding to the certified public key that was communicated to the second component. Other techniques for verifying the identity of a compliant device, common in the art, may alternatively be used. In a preferred embodiment, the challenge-response process includes a time-out limit at each stage, to detect an attempt of copying protected material from a remote source, for example, from a remote Internet site. A local extraction and distribution component can be expected to provide a response to a challenge within microseconds, whereas a remote component might be expected to require milliseconds or more to communicate the response back to a remote challenging device.

Note that if another extraction source 180 is not a compliant device, the authentication process discussed above will fail, as indicated by the dashed arrow 150', and the distribution module 120 will not accept content material from this source 180.

After authenticating that the distribution module 120 is a compliant module, the extraction device 110 transmits the extracted content material and digitally signs the transmission. The compliant distribution module 120 does not accept content material for further distribution unless the digital signature of the content material corresponds to the signature of the authenticated extraction device 110. In this manner, if an alternative source 180 attempts to substitute material, as indicated by the dashed line 181, after the compliant extraction device satisfies the authentication process, the compliant module 120 will

recognize the substitution, because the substituted material will not be digitally signed by the extraction module 110. In a preferred embodiment, a one-time key is used, to prevent repeated use, or a secure time-stamp is used, to assure that the signed material is from a recently challenged extraction device.

Other security techniques can also be used to assure that the binding between the device 110 and module 120 remains secure. FIG. 3 illustrates an example block diagram of an extraction device 110 and distribution module 120 that provides a secure communication of content material. The binders 330 and 350 in the extraction device 110 and distribution module 120, respectively, effect the above discussed cryptographic authentication process, and generate a set of secure keys, Key1 and Key1'. A cryptographic key exchange, such as a Diffie-Hellman exchange, common in the art, is preferably used to provide an encryption key, Key1, for use by the extraction device 110, and a decryption key, Key1', for use by the distribution module 120. The keys Key1 and Key1' may be identical, or may each be a corresponding key of an asymmetric key-pair. The extraction device 110 encrypts the extracted content material using the exchanged key, Key1, which is commonly termed a "session key". In a preferred embodiment, the distribution device 120 stores the encrypted material, and also stores the session key that was used to encrypt the encrypted material. Thereafter, the distribution module 120 can decrypt the encrypted material as required, using the stored session key, Key1', that is associated with the stored encrypted material, via a decrypter 370. An optional renderer 380 is configured to render the decrypted content material for a direct presentation to a user.

Also in a preferred embodiment, the playback device 140 is configured to decrypt the extracted content material. In this embodiment, the distribution module 120 encrypts the session key Key1' using a second session key, Key2, that is established between the module 120 and the playback device 140, via the encrypter 360. The encrypted content material and the re-encrypted original session key are thereafter communication to the playback device 140. The playback device 140 decrypts the encrypted original session key, using the second session key Key2, and then decrypts the encrypted extracted content material, using this decrypted session key Key1'. Alternatively, the decrypted content material from the decrypter 370 is re-encrypted by the encrypter 360 using the second session key Key2, and the playback device 140 is configured to decrypt this re-encrypted content material directly.

Another method of binding the extraction device 110 to the distribution module 120 is to physically bind the devices, as illustrated in FIG. 2. In the alternative

embodiment of the system 100' in FIG. 2, a compliant extraction device 110' is physically bound to a distribution module 120'. Any of a variety of techniques can be employed to assure the security of this bonding. In a preferred embodiment, the system 100' includes a tamper-detection device, such as a frangible device that is attached to an enclosure that binds the components 110' and 120'. Alternatively, an integrated circuit can be created that includes the output stage of the extraction device 110' and the input stage of the distribution module 120', so that the actual interface point between the two devices 110' and 120' is not accessible for inserting a substitute, potentially illicit, copy of copy protected material. Another alternative is to merely rely on the lack of an explicit interface port to discourage the "casual" theft of copy protected material via a download from an Internet site. That is, if the extraction device 110' and distribution module 120' are within a single enclosure, with no obvious or external interconnect point, most consumers will not open the enclosure, decipher the layout to determine the interface point, and modify the circuit board to allow for an insertion of an illicit copy of a song. Contrarily, unplugging a legitimate source and plugging in an illicit source via external connections between components 110, 120, such as illustrated in FIG. 1, can be considered a reasonably likely occurrence.

In like manner, if the extraction device 110' is a software application, such as an application that reads content material from a CD or DVD on a personal computer, and conventionally stores a compressed file, such as an MP3 file, on a hard drive, then, in accordance with this aspect of the invention, the distribution module 120' is included within the same software application. In this manner, the material that is stored on the hard drive is bound to the distribution module 120', preferably in an encrypted form. Thereafter, the distribution module 120' provides material to other playback or recording devices 140 if and only if the material on the hard drive corresponds to material that has been bound to the device 120'. In this manner, material that is placed on the hard drive via another source 180, such as an Internet connection, will not be distributed by the distribution module 120'.

In a further embodiment of this invention, the binding process occurs at one point in time, and the actual communication of the material occurs at a later time. A time limit may still be employed during the authentication process, to verify that the extraction device 110 and distribution module 120 are in close physical proximity, but thereafter, the extraction device 110 is configured to allow substantially unrestricted communication of protected material to the previously verified module 120, using, for example, the key Key1 for all subsequent encodings. In like manner, the extraction device 110 may be configured to grant an automatic authentication of the first distribution module 120 that it encounters,

thereby minimizing the complexity required for effecting the binding between the extraction device 110 and the distribution module 120. In this embodiment, the extraction device 110 is preferably configured to provide protected material only to the first module 120 that it encounters, thereby precluding the use of the extraction device 110 as a provider of widely distributable copies of the material. That is, for example, when a user acquires an extraction device 110, and connects it to a distribution module 120, the initial connection is automatically verified relative to the this module 120, thereby facilitating an easy-to-use and highly-reliable configuration of the extraction device to a user's environment. Thereafter, however, the user is prevented from using this extraction device to provide material to other users' distribution devices. To allow for a subsequent change to the user's system, a one-for-one replacement protocol is provided that allows the replacement of the distribution device 120 by another distribution device, wherein, after the replacement, a subsequent attempt to use the original device 120 with the extraction device 110 will fail. In a preferred embodiment, the identifier of the original device 120 is placed in a "revoked identifier" list maintained by the extraction device 110 after the replacement.

In each of the above embodiments, the extraction device 110 may also be configured to access an external source of revoked authorization identifiers. Such revoked authorizations may be issued when it is discovered that unauthorized copies of the content material originated at the identified device. Copending U.S. patent application "UPDATING A REVOCATION LIST TO FOIL AN ADVERSARY", serial number 09/370,489, filed 9 August 1999 for Michael Epstein, Attorney Docket PHA 23,743 describes a method and system for distributing lists of revoked authorization identifiers of devices, and is incorporated by reference herein.

The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise various arrangements which, although not explicitly described or shown herein, embody the principles of the invention and are thus within its spirit and scope. For example, some copy protection schemes rely on the use of a "ticket" that is "punched" at each level of a copy hierarchy. European patent EP0906700, "METHOD AND SYSTEM FOR TRANSFERRING CONTENT INFORMATION AND SUPPLEMENTAL INFORMATION RELATED THERETO", issued 7 April 1999 to Johan P.M.G. Linnartz et al, presents a technique for the protection of copyright material via the use of a watermark "ticket" that controls the number of times the protected material may be rendered, and is incorporated by reference herein. This ticketing scheme can be incorporated in this invention by configuring the extraction device 110 to also

"punch" the ticket, and to provide a certified copy of this ticket to the distribution module 120. Alternatively, if the distribution module 120 provides an identifier, the identifier and the ticket can be signed together by the extraction device 110. In this manner, other distribution devices are able to detect an attempted reuse of a signed ticket. These and other system configuration and optimization features will be evident to one of ordinary skill in the art in view of this disclosure, and are included within the scope of the following claims.

CLAIMS:

1. A system (100) comprising:

an extraction device (110) that is configured to receive protected content material and to provide therefrom an extracted data item corresponding to at least a portion of the protected content material, and

a distribution module (120) that is configured to receive the extracted data item from the extraction device (110), and to store the extracted data item for subsequent communication to a playback device (140),

wherein

the extraction device (110) is bound to the distribution module (120) so as to prevent an acceptance of an unauthorized data item by the distribution module (120) from a source other than the extraction device (110) or another bound device.

2. The system (100) of claim 1, wherein

the extracted data item that is stored by the distribution module (120) is bound to the distribution module (120).

3. The system (100) of claim 1, wherein

the extraction device (110) and distribution module (120) are bound via a physical connection.

4. The system (100) of claim 1, wherein

the extraction device (110) and distribution module (120) are bound via a cryptographic process.

5. The system (100) of claim 4, wherein

the cryptographic process includes a timeout limit.

6. The system (100) of claim 1, wherein

the extraction device (110) is further configured to compress the portion of the content material to form the extracted data item.

7. An extraction device (110) comprising:

an extractor (310) that is configured to extract at least a portion of copy protected material from an original source (101) to form an extracted data item and

a binder (330) that is configured to bind the extracted data item to a subsequent receiving device (120).

8. The extraction device (110) of claim 7, wherein

the binder (330) includes

an authentication device that is configured to verify that the subsequent receiving device is a device that is compliant with a copy protection standard, and

the binder (330) binds the extracted data item to the subsequent receiving device (120) based on the verification of the subsequent receiving device (120).

9. The extraction device (110) of claim 7, further including

a signing device that is configured to digitally sign the extracted data item.

10. he extraction device (110) of claim 9, wherein

the signing device is further configured to digitally sign a copy-limiting ticket that is associated with the copy protected material.

11. he extraction device (110) of claim 7, further including

an encryption device (320) that is configured to encrypt the extracted data item.

12. he extraction device (110) of claim 11, wherein

the encryption device (320) encrypts the extracted data item based on a session key that is dependent upon a parameter provided by the subsequent receiving device (120).

13. he extraction device (110) of claim 7, wherein

the extractor (310) is further configured to compress the portion of the content material to form the extracted data item.

14. distribution module (120) that is configured to receive protected content material from an extraction device (110), comprising

a binder (350) that is configured to verify that the received protected content material is bound to the distribution module (120).

15. he distribution module (120) of claim 14, wherein

the binder (350) is configured to verify a digital signature associated with the protected content material, and

the distribution module (120) provides the protected content material to a subsequent receiver (140) based on the verification of the digital signature.

16. he distribution module (120) of claim 14, further including

an encryption device (360) that is configured to encrypt the protected content material.

17. he distribution module (120) of claim 14, wherein

the extraction device (110) encrypts the protected content material based on a session key that is dependent upon a parameter provided by the distribution module (120), and

the distribution module (120) further includes

an encryption device (360) that is configured to encrypt the session key.

18. he distribution module (120) of claim 14, wherein

the extraction device (110) encrypts the protected content material based on a session key that is dependent upon a parameter provided by the distribution module (120), and

the distribution module (120) further includes

a decryption device (370) that is configured to decrypt the encrypted copy protected material based on the session key.

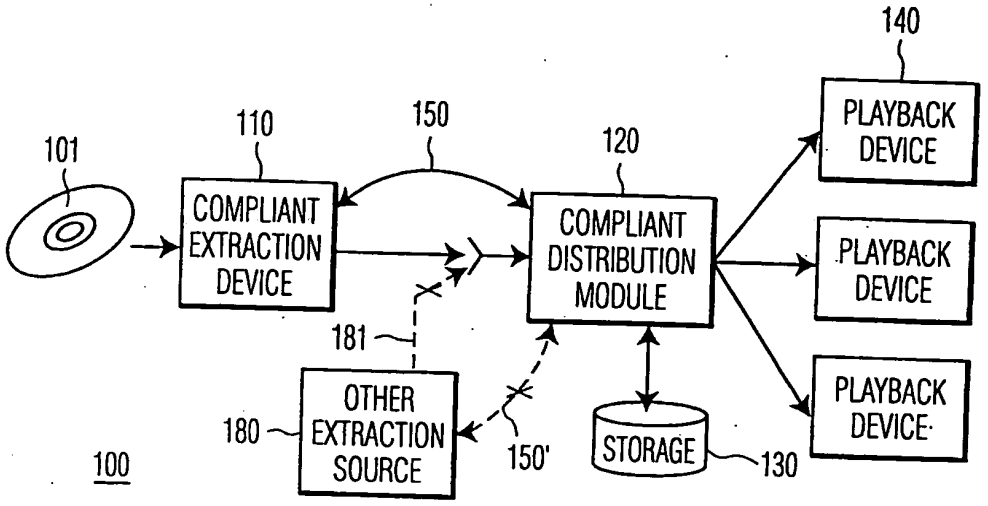

140
PLAYBACK DEVICE
110
150
120
101
COMPLIANT EXTRACTION DEVICE
COMPLIANT DISTRIBUTION MODULE
PLAYBACK DEVICE
PLAYBACK DEVICE
181
OTHER EXTRACTION SOURCE
180
150'
STORAGE
130
100

FIG. 1

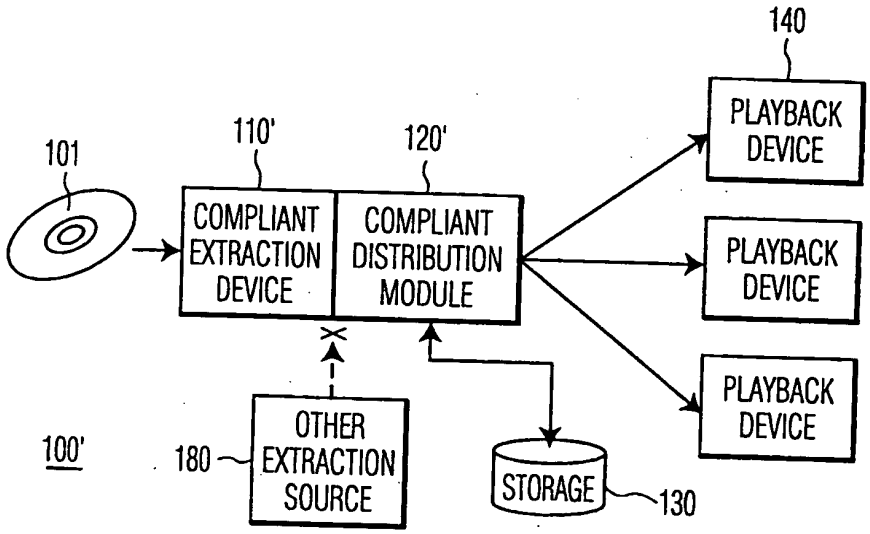

140
PLAYBACK DEVICE
110'
120'
101
COMPLIANT EXTRACTION DEVICE
COMPLIANT DISTRIBUTION MODULE
PLAYBACK DEVICE
PLAYBACK DEVICE
OTHER EXTRACTION SOURCE
100'
180
STORAGE
130

FIG. 2

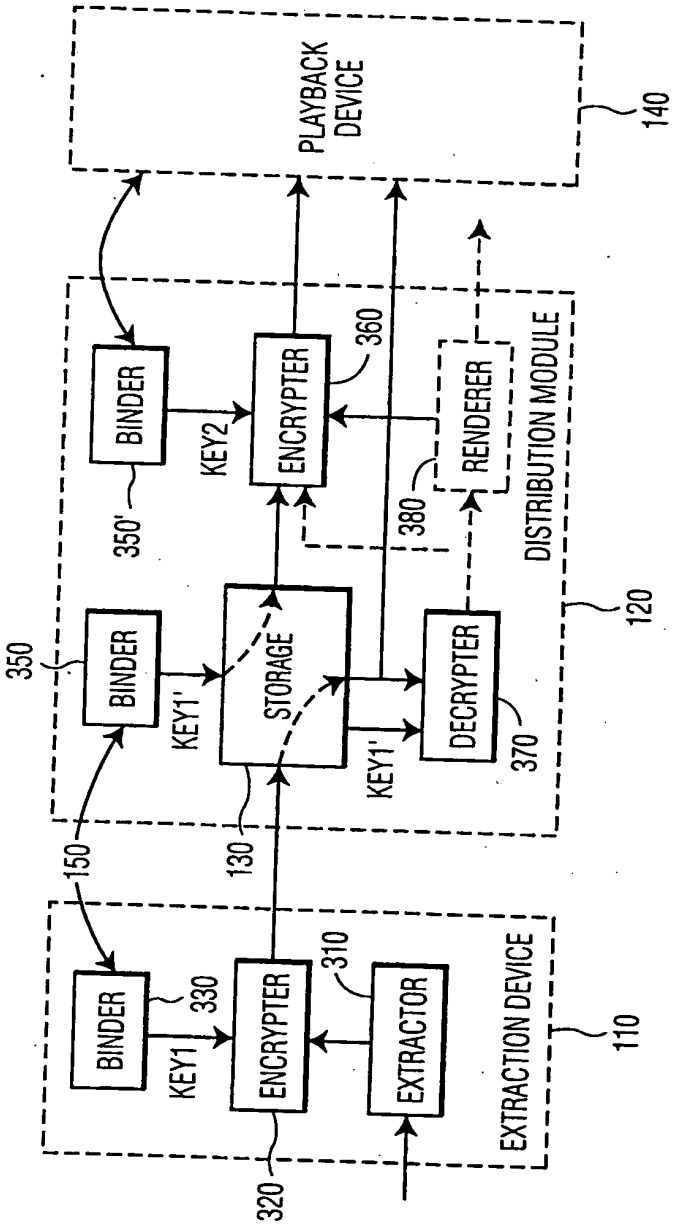

PLAYBACK DEVICE
140
DISTRIBUTION MODULE
120
BINDER
350'
KEY2
ENCRYPTER
360
RENDERER
380
BINDER
350
KEY1'
STORAGE
DECRYPTER
370
KEY1'
150
130
BINDER
330
KEY1
ENCRYPTER
310
EXTRACTOR
EXTRACTION DEVICE
110
320

FIG. 3

INTERNATIONAL SEARCH REPORT

Int ational Application No
PCT/EP 00/13227

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G10H1/00 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G10H G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 476 746 A (JANSSENS WILHELMUS ET AL) 19 December 1995 (1995-12-19) column 2, line 34 - line 43 column 4, line 10 - line 54 column 7, line 49 - line 57 column 9, line 1 - line 7 column 10, line 53 - line 67; figures 1-3,10	1-18
A	WO 99 66386 A (WIMMER CARL P ;AHMADI BABAK (CA)) 23 December 1999 (1999-12-23) page 11, line 13 -page 12, line 2 page 16, line 16 -page 17, line 13 page 22, line 16 -page 23, line 9; claim 1; figure 9	1-18

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 March 2001	04/04/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Pulluard, R

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int tional Application No
PCT/EP 00/13227

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 933 503 A (BERSON THOMAS A ET AL) 3 August 1999 (1999-08-03) column 14, line 45 -column 15, line 5 column 16, line 25 - line 61; figures 3,4	1-4,7-9, 14-18
A	US 5 636 276 A (BRUGGER ROLF) 3 June 1997 (1997-06-03) column 2, line 1 - line 55	1,4,6-8, 11,13

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int ational Application No
PCT/EP 00/13227

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5476746 A	19-12-1995	EP 0578870 A	19-01-1994
		AT 146135 T	15-12-1996
		AT 147017 T	15-01-1997
		DE 69215864 D	23-01-1997
		DE 69215864 T	19-06-1997
		DE 69307037 D	13-02-1997
		DE 69307037 T	26-06-1997
		EP 0579299 A	19-01-1994
		JP 6092045 A	05-04-1994
		JP 6092046 A	05-04-1994
		US 5366951 A	22-11-1994
		US 5616697 A	01-04-1997
		AT 147016 T	15-01-1997
		DE 69307036 D	13-02-1997
		DE 69307036 T	26-06-1997
		EP 0579297 A	19-01-1994
		JP 6108380 A	19-04-1994
		US 5510225 A	23-04-1996
WO 9966386 A	23-12-1999	NONE	
US 5933503 A	03-08-1999	NONE	
US 5636276 A	03-06-1997	DE 4413451 A	14-12-1995
		AT 169762 T	15-08-1998
		DE 59503112 D	17-09-1998
		DK 678851 T	17-05-1999
		EP 0678851 A	25-10-1995
		ES 2119344 T	01-10-1998
		GR 3027730 T	30-11-1998